🔧 Ejercicio Práctico: Escaneo de Subred con Detección de Servicios y Reporte

---

📝 Descripción

Este ejercicio consiste en automatizar un escaneo de red sobre una subred local, detectar los servicios que corren en puertos abiertos, identificar versiones de software y generar un resumen legible para ser utilizado en un reporte técnico.

🎯 Objetivos de aprendizaje

- Automatizar el escaneo de una red completa (ej. `192.168.1.0/24`).
- Detectar **puertos abiertos y versiones de servicios** (`-sV`).
- Identificar **hosts activos**.
- Estructurar e imprimir los resultados de forma clara.
- Reflexionar sobre los servicios expuestos y su posible impacto en la seguridad.

👨‍💻 Instrucciones

1. Asegúrate de tener instalado:
    - `nmap`
    - la librería `python-nmap`
2. Crea un script en Python que:

- Realice un escaneo con `-sV` sobre la subred `192.168.1.0/24` (puedes ajustar a la IP de tu entorno).
- Detecte y liste:
  - IP del host
  - Puerto abierto
  - Nombre del servicio
  - Versión del software si está disponible

3. Imprima un resumen ordenado por host, como si se preparara para un informe de pentesting.
4. Asegúrate de ejecutar este ejercicio **únicamente en redes de laboratorio o con autorización expresa**.

📌 Formato sugerido de salida:

Host: 192.168.1.10
- Puerto 22: ssh (OpenSSH 7.6)
- Puerto 80: http (Apache httpd 2.4.29)

Host: 192.168.1.15
- Puerto 139: netbios-ssn
- Puerto 445: microsoft-ds

Total de hosts activos: 2

⚖️ Consideraciones Éticas

- No se deben ejecutar escaneos en redes públicas ni entornos productivos sin consentimiento explícito.
- Este ejercicio es válido solo en entornos de prueba controlados.
- Documentar y validar con tu instructor o equipo antes de escanear redes compartidas.
